Scientific Research Publishing

Advances in Internet of Things, 2023, 13, 109-118
https://www.scirp.org/journal/ait
ISSN Online: 2161-6825
ISSN Print: 2161-6817

Cybersecurity and Privacy Protection in Vehicular Networks (VANETs)

Bruno Macena, Celio Albuquerque, Raphael Machado

Instituto de Computação, Universidade Federal Fluminense (UFF), Rio de Janeiro, Brazil
Email: brunomacena@id.uff.br, celioalbuquerque@id.uff.br, raphaelmachado@ic.uff.br

How to cite this paper: Macena, B., Albuquerque, C. and Machado, R. (2023) Cybersecurity and Privacy Protection in Vehicular Networks (VANETs). *Advances in Internet of Things*, **13**, 109-118.
https://doi.org/10.4236/ait.2023.134006

Received: September 1, 2023
Accepted: October 27, 2023
Published: October 30, 2023

Abstract

As Vehicular ad hoc networks (VANETs) become more sophisticated, the importance of integrating data protection and cybersecurity is increasingly evident. This paper offers a comprehensive investigation into the challenges and solutions associated with the privacy implications within VANETs, rooted in an intricate landscape of cross-jurisdictional data protection regulations. Our examination underscores the unique nature of VANETs, which, unlike other ad-hoc networks, demand heightened security and privacy considerations due to their exposure to sensitive data such as vehicle identifiers, routes, and more. Through a rigorous exploration of pseudonymization schemes, with a notable emphasis on the Density-based Location Privacy (DLP) method, we elucidate the potential to mitigate and sometimes sidestep the heavy compliance burdens associated with data protection laws. Furthermore, this paper illuminates the cybersecurity vulnerabilities inherent to VANETs, proposing robust countermeasures, including secure data transmission protocols. In synthesizing our findings, we advocate for the proactive adoption of protective mechanisms to facilitate the broader acceptance of VANET technology while concurrently addressing regulatory and cybersecurity hurdles.

Keywords

Vehicular Ad-Hoc Networks (VANETs), Privacy and Data Protection, Cybersecurity, Pseudonymization Schemes, Internet of Vehicles (IoV)

1. Introduction

Vehicular networks (VANETs), evolved from mobile ad hoc networks (MANETs) principles, enable spontaneous wireless communication between vehicles. Their emergence has ignited discussions about the security and privacy implications for vehicles and their occupants. With VANETs differing significantly from other Ad Hoc networks, particularly in their reliance on security and privacy due to the potential ramifications of control failures [1], there is an urgent need to ensure the confidentiality of sensitive information, which includes data like unique identifiers, routes, positions, and even insights into the probable vehicle model [2].

Privacy is universally acknowledged as a fundamental human right, anchored in the ethos of the "right to be let alone" [3] [4]. This foundational right, emphasizing freedom from interference and the liberty to associate freely, is enshrined in numerous global regulations. Issued by the United Nations in 1948, The Universal Declaration of Human Rights explicitly addresses rights against unwarranted intrusions into individual privacy [3]. Nations worldwide have tailored their regulatory frameworks to protect these rights, with U.S. states such as California enacting their privacy protections [5] and broader federal instruments like the Divers Privacy Protection Act (DPPA 2015) coming into force.

The GDPR—General Data Protection Regulation emphasizes the right to privacy in Europe, advocating for robust security measures, including pseudonymization and encryption [6] [7]. Meanwhile, Brazil's General Personal Data Protection Law (LGPD) mirrors much of the GDPR, emphasizing personal data protection [8]. Such global legislative endeavors underscore the importance and complexity of data privacy.

However, navigating this multifaceted regulatory landscape is challenging, especially for technologies like VANETs. The potential for conflicts between international jurisdictions and the daunting intricacy of cross-border regulations further complicates matters. Nevertheless, the need for robust privacy safeguards in VANETs is undeniable. The technology's inherent nature exposes a wealth of sensitive information, making it vulnerable to various cybersecurity threats.

This article addresses the challenges inherent in VANETs within the prevailing regulatory environment. By exploring conceptual countermeasures and evaluating existing protection mechanisms, we aim to advocate for strategies that bolster security in VANETs, facilitating their broader adoption by ensuring data protection and mitigating regulatory challenges.

2. Literature Review

Vehicular Ad Hoc Networks (VANETs) introduce a unique paradigm in vehicular communication, promising enhanced road safety and traffic efficiency. However, they also present challenges, especially in security and privacy. A primary concern is the potential misuse of historical location data, which, if mishandled, can have vast implications, hindering the adoption of VANET technology.

Differing approaches to privacy in VANETs include policy-based and anonymity-based schemes. Vehicles articulate their privacy preferences in policy-based setups, trusting Location-Based Services (LBSs) to comply [9]. These LBSs, which offer services ranging from safety alerts to roadside assistance, are responsible for adhering to privacy policies and regulatory norms.

Pseudonymization schemes, a subset of anonymity-based strategies, can be rooted in public key or identity-based cryptography. An example to consider is the Density-based Location Privacy (DLP) scheme [10], which this article emphasizes for its clear advantages. Numerous other pseudonymization strategies, like K-anonymity [11], Assignment Dynamic MAC/PHY Address with shuffle (DMAS) [12] [13], Mix-Zone (CMIX) [14], and AMOEBA [9] combined with Random silence period [15], present viable alternatives in this context. Subsequent sections delve into these protocols and algorithms, highlighting the ongoing community research. Regarding cybersecurity-related concerns, this article references detailed issues and their counter measures [16] [2].

3. Research Methodology

In this article, we employed a survey-based methodology grounded in literature reviews to delve into the multifaceted challenges and intricacies of privacy, security, and regulatory related dimensions within Vehicular Ad Hoc Networks (VANETs) and the broader Internet of Vehicles (IoV) ecosystem. Our approach prioritized the identification and analysis of relevant academic publications in VANETs' privacy and security, ensuring that our selected sources were academically recognized and frequently cited.

Our research unearthed key findings and challenges, particularly emphasizing the relevant role of pseudonymization in navigating the intricate regulatory landscapes. This synthesized narrative, derived from our methodological approach, clarifies current challenges, and serving as a beacon for future inquiries in this dynamic domain.

4. Privacy Schemes for Location Protection in VANETs

In VANETs, the potential misuse of historical location data poses significant privacy concerns. Various schemes have been devised to address these challenges, from policy-based approaches relying on Location-Based Services (LBSs) to anonymity-driven strategies. As stated before, this article focuses on anonymity-based solutions, particularly pseudonymization techniques, as they offer clear advantages in mitigating regulatory implications and bolstering community trust in VANET technology.

4.1. AMOEBA

One of the most relevant proposals to address this problem of unauthorized tracking is the privacy scheme for location in VANETS called AMOEBA [9]. AMOEBA uses the concept of a navigation group for V2I (Vehicle-to-Infrastructure) communications to anonymize access to the VANET's location service. AMOEBA introduces a random silent period between pseudonym updates for V2V (Vehicle-to-vehicle) communications.

As for anonymization, in this case, pseudonymization, consider that the objective is to mask the identifiers of a legitimate node throughout its navigation, generating new pseudonyms periodically according to the methodology of the adopted anonymization protocol.

AMOEBA has, by definition, the problem of the mitigation of vehicle location tracking, minimizing the possibility of node profiling through the use of Location Based Services—LBSs, of service providers accessed by vehicles [9].

For better understanding, consider that an LBS application captures the most recent location of vehicles that are customers of this service in a VANET and uses them to provide services requested, such as the query to locate a specific store close to its last location.

In AMOEBA, the road network is divided into two zones. These are the observed and unobserved zones from an opponent's point of view. In the observed zones, the adversary could track the location of target vehicles. On the other hand, in unobserved zones or mixing zones, it is the opposite because an opponent cannot perform location tracking. These unobserved zones are predetermined locations where vehicles vary their directions, speeds, and aliases. Generally, road intersections are used for this category. Thus, opponents would have difficulty linking vehicles from one zone to another [10].

Thus, to avoid this profiling of nodes through access to LBS services, it is necessary to provide unlinking between the pseudonyms of the nodes and the LBS applications. Moreover, to ensure the effectiveness of the anonymization mechanism, AMOEBA applies the concept of navigation groups, providing the decoupling between the location of access to the LBS application and the LBS application itself through a figure of the leader of the navigation group, this being a proxy for anonymous access to other group members (legitimate neighboring nodes in a VANET). This solution protects user privacy even if the vehicle is tracked. This is because, without adopting this group concept, a vehicle is uniquely associated with the V2I (Vehicle to Infrastructure) platform. This tracking would be possible through geographic information and estimation of the node's location when the LBS service request is transmitted within a specific period in a specific observed and identified area.

In the case of V2V (Vehicle to Vehicle) communications, AMOEBA uses the random silent period [15] to update aliases in communications, which are related to BSM (Basic Security Messages) broadcast messages transmitted to neighboring nodes. By simply updating a pseudonym, it is still possible for a legitimate node (vehicle) to be tracked, as the temporal and spatial relationship between new and old vehicle locations remains correlated between new and old pseudonyms. At this point, the random silence period between pseudonym updates ensures that the vehicle remains silent for a randomly chosen period, sufficient to promote the unlinking of vehicles in the VANET.

Furthermore, this concept extends to the AMOEBA proposal to use the already mentioned concept of Navigation Groups, taking advantage of the restrictions of spatial dependence and geographic proximity, flow direction, and temporal characteristics of a specific group and defining a group leader randomized by specific rotation protocol.

A seemingly obvious limitation of the application of this navigation group concept would be that the node elected as leader would suffer computational overhead for the execution of group protocols, in addition to the fact that the leader would sacrifice its location privacy by continually revealing it in the V2I applications, until the next periodic leader rotation.

4.2. Cryptographic MIX-Zone or CMIX

In the cryptographic mixing zone (Cryptographic MIX-zone or CMIX) [14], certification authorities (CAs) are used through RSUs (Road-side Units) to provide vehicles within a mixing zone with a public and private key pair (Vehicular Public Key Infrastructure—VPKI). These keys are used to encrypt all messages while inside the mixing zone. Moreover, it is also used to exchange pseudonyms as part of the services of this V2I zone (Vehicle to Infrastructure) together with the RSU (Road Side Unit) and the CA (Certification Authority) or PCA (Pseudonym Certification Authority) and digitally sign pseudonyms for authenticity and identity authentication.

There are considerations for adopting hardware cryptographic modules (Hardware Security Module—HSM) and cryptographic device tamper protections (Tamper Proof Protection) as solutions. However, due to the high related costs, they can make a deployment initiative financially unfeasible. Other relevant issues are on account of the VPKI (Virtual Public Key Infrastructure) hierarchy for cross-certification and reliability of the signature mechanism and the certificates themselves (for example, the PCA must not alone know the identity and pseudonym of the nodes, providing shared custody with segregation of duties in its infrastructure). In addition to the mechanism for generating random aliases, its temporal validity, variability within the universe of beacons (Cooperative Awareness Messages—CAMs) to be transmitted, and the certificate revocation process. Additionally, considerations about the rotation of certificates by nodes can provide greater privacy based on location, decreasing the possibility of correlation of aliases between different locations (different blending zones).

4.3. K-Anonymity

K-anonymity [11] is a scalable approach to protecting node privacy when using location-based services (LBSs). It is accomplished by using a customizable framework for privacy requirements, allowing each legitimate node to specify its minimum level of anonymity and maximum temporal and spatial tolerances when requesting services from LBSs.

This level of anonymity is translated by a K variable, which is customizable. In location k-anonymity, a node is considered k-anonymous only if the location information sent to a Location-based Service is indistinguishable from at least $k - 1$ other node's location information. Thus, a larger k in location anonymity implies more excellent guarantees of location privacy. The approach considers removing identities and the Spatio-temporal camouflage of location information. Such an approach uses an architecture that inserts a trusted central server for the anonymization service. This acts as a security gateway for legitimate nodes to access LBS services. This security gateway runs a set of location perturbation algorithms.

In this way, messages sent to LBS providers are handled by the anonymity security gateway that removes any identifiers, such as IP addresses. It disrupts the location information through Spatio-temporal cloaking and then forwards the anonymized message to the LBS provider.

In the K-anonymity approach, a node transmits its spatial position information when the number of nodes within its range is more significant than a certain customizable threshold (K). The node only transmits the beacon message once several other nodes have visited the exact location.

4.4. Dynamic Change MAC/PHY

Dynamic change MAC/PHY addresses on WIFI networks aim to protect the location and privacy of legitimate nodes in VANETs (vehicles, their drivers, and other occupants). It is worth mentioning the protection strategy based on the periodic updating of interface identifiers, among which the Assignment Dynamic MAC/PHY Address with shuffle (DMAS), where the node dynamically swaps its assigned MAC/PHY addresses.

This strategy takes advantage of the postulates related to the MIX Zones strategy previously exposed in this article, adding components for randomization of MAC/PHY link-layer addresses, using the same idea of dynamic IP addressing of the DHCP protocol.

The simple adoption of such a protocol confers the exchange of network-layer identifiers concomitantly [13]. The dynamic MAC/PHY address assignment with scrambling still considers authentication mechanisms for wireless access based on the cryptographic key exchange.

4.5. Density-Based Location Privacy—DLP

The Density-based Location Privacy (DLP) [10] approach to privacy protection presents itself as a better-performing alternative, reducing the probability of successful tracking of a node by an adversary than in the Mix-Zone and AMOEBA schemes with a random silent period, already presented in this article.

The DLP approach uses the density of neighboring nodes as a threshold for changing aliases, as in the K-Anonymity approach previously presented.

DLP derives the delay distribution and the average total delay of a node within a density zone. It also considers the dynamic MAC/PHY address assignment approach with scrambling for a dynamic exchange of TCP/IP stack identifiers, as presented earlier as IP and MAC/PHY addresses.

This method operates because each node is pre-equipped with an ample set of pseudonyms. A pseudonym switch is only initiated when the count of neighboring nodes surpasses k − 1, where k is a customizable parameter. In essence, DLP ensures privacy by stipulating that a node can only alter its pseudonym if at least k − 1 nodes are in its vicinity.

In this approach, the probability of successful location tracking of a target node by an adversary is inversely proportional to the traffic intensity and the variation in the speed of the nodes (vehicles).

5. Cybersecurity Issues and Countermeasures

Vehicular Networks (VANETs) have some relevant known Cybersecurity Issues [16], in which adversaries can exploit a range of tactics to undermine network integrity and expose identity data. Some relevant Attack methods are:

Fake Alerts: False Decentralized Environmental Notification Messages (DENM) can disrupt road operations. Such misinformation may involve fake traffic conditions or Cooperative Awareness Messages (CAM) containing falsified vehicle data. Authenticating messages using cryptographic schemes, like the Elliptic Curve Digital Signature Algorithm (ECDSA), is crucial for counteracting this.

Data Theft: Attackers might deploy rogue wireless access points or impersonate legitimate network nodes to capture sensitive network packets, including DENMs and CAMs. Countermeasures include encryption, authentication, and efficient key management.

Unauthorized Profiling: Personal data for demographic profiling or targeted advertising can be misused. Pseudonymous solutions, as discussed earlier, offer mitigation.

Illusion Attacks: Deliberate broadcasting of incorrect road traffic warnings can cause accidents or traffic congestion. A Plausibility Validation Network (PVN) can validate or discard such messages [17].

Fake Identity & Impersonation: Both involve adversaries sending messages while pretending to be legitimate vehicles. These attacks can degrade safety or exploit system benefits, like free passage. Cryptographic message authentication and ID-based cryptographic solutions are essential countermeasures.

Vehicular Networks (VANETs) offer transformative road traffic management and communication potential. However, the impact of cybersecurity threats, such as Data Theft, and Unauthorized Profiling, raises serious data protection and integrity concerns. Effective countermeasures like the Elliptic Curve Digital Signature Algorithm (ECDSA), encryption, and pseudonymous solutions are vital to safeguard against these issues. As VANETs evolve, striking a balance between technological advancement and robust security measures becomes paramount to ensure their successful and trusted integration into transportation systems.

6. Contribution and Conclusions

This article presents the research results around Privacy Protection and Cybersecurity in vehicular Ad Hoc networks. It presents the motivators in terms of regulatory aspects and the prevention of Cyber Risks as arguments to benefit the adoption of VANETs by the community and public or private entities.

Evaluating the known problems in terms of Cybersecurity and Privacy Protection directly related to VANETs brings a reflection on the known attacks and their implications. This article also presents and discusses the protection approaches as known countermeasures.

The main contribution of this work is to demonstrate the importance of adopting a pseudonymization approach to minimize data protection regulatory requirements. By adopting an efficient anonymization scheme, the number of compliance requirements translated into data protection controls, as expected by most data privacy laws and regulations, can be drastically reduced, which can be achieved using the location privacy protection method based on vehicle density zones. It considers the adoption of mixing zones as a point of interest for processing the algorithms. It takes advantage of the techniques postulated in K-anonymity and the exchange of identifiers in the network and link layers. This set can mitigate the vehicle location problem through this pseudonym change, based on a threshold on the count of neighboring vehicles within a density zone.

This article also explores several known Cybersecurity attacks on VANETs that directly address privacy protection challenges. It presents approaches capable of eliminating malicious nodes and adopting secure data transmission protocols, including message authentication between vehicles considered legitimate nodes.

Some relevant questions should be raised and would be the target of future research works, questions about where cryptographic keys and pseudonyms should be stored on the node (Vehicle). Moreover, around the considerations for adopting Hardware cryptographic Security Modules—HSMs. An around cryptographic device tamper protections (Tamper-Proof Protection) that can, while being apparent solutions, make a deployment initiative financially unfeasible.

Expanding on this work, discussions and future research should address the constraints of computational delays potentially generated using cryptographic mechanisms in networks that depend on the sensitivity of the response time for the quality of services, especially for BSMs.

Furthermore, potentially carrying out the evaluation and proposing an approach to K, automatically calculated in a self-adaptive, considered optimal for the identifiable traffic conditions on the highway, so anonymity remains guaranteed without the need for manual and dynamic interference from the application's user.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Wiedersheim, B., Ma, Z., Kargl, F. and Papadimitratos, P. (2010) Privacy in

Inter-Vehicular Networks: Why Simple Pseudonym Change Is not Enough. 2010 Seventh International Conference on Wireless On-demand Network Systems and Services (WONS), Kranjska Gora, 3-5 February 2010, 176-183, https://doi.org/10.1109/WONS.2010.5437115

[2] https://ieeexplore.ieee.org/abstract/document/5437115

[3] Al-Kahtani, M.S. (2012) Survey on Security Attacks in Vehicular Ad Hoc Networks (vanets). In 2012 6*th International Conference on Signal Processing and Communication Systems*, Gold Coast, 12-14 December 2012, 1-9. https://doi.org/10.1109/ICSPCS.2012.6507953

[4] United-Nations (1948) Universal Declaration of Human Rights. United Nations Portal. https://www.un.org/en/about-us/universal-declaration-of-human-rights

[5] Warren, S.D. and Brandeis, L.D. (1890) The Right to Privacy. *Harvard Law Review IV*, **4**, 193-220. https://www.jstor.org/stable/1321160

[6] California (2018) California Consumer Privacy Act CCPA. California Legislative Information, California Law, The Civil Code of California, CIV. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

[7] European-Union (2016) General Data Protection Regulation—GDPR. European Data Protection Supervisor—EDPS. https://gdpr-info.eu/

[8] Teixeira, G.A., da Silva, MM. and Pereira, R. (2019) The Critical Success Factors of GDPR Implementation: A Systematic Literature Review. *Digital Policy*, *Regulation and Governance*, 21, 402-418. https://www.emerald.com/insight/content/doi/10.1108/DPRG-01-2019-0007/full/html

[9] LGPD (2019) Brazil Data Protection Law. General Secretariat of the Presidency of the Republic Sub-Chief for Legal Affairs. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm#:~:text=1%C2%BA%20Esta%20Lei%20disp%C3%B5e%20sobre,da%20personalidade%20da%20pessoa%20natural

[10] Sampigethaya, K., Li, M., Huang, L. and Poovendran, R. (2007) Amoeba: Robust Location Privacy Scheme for VANET. *IEEE Journal on Selected Areas in Communications*, **25**, 1569-1589. https://doi.org/10.1109/JSAC.2007.071007

[11] Song, J.-H., Wong, V.W.S. and Leung, V.C.M. (2009) Wireless Location Privacy Protection in Vehicular Ad-Hoc Networks. 2009 *IEEE International Conference on Communications*, Dresden, 14-18 June 2009, 1-6. https://doi.org/10.1109/ICC.2009.5199575

[12] Gedik, B. and Liu, L. (2007) Protecting Location Privacy with Personalized K-Anonymity: Architecture and Algorithms. *IEEE Transactions on Mobile Computing*, **7**, 1-18. https://doi.org/10.1109/TMC.2007.1062

[13] Lei, M., Qi, Z., Hong, X. and Vrbsky, S.V. (2007) Protecting Location Privacy with Dynamic Mac Address Exchanging in Wireless Networks. In 2007 *IEEE Intelligence and Security Informatics*, New Brunswick, 23-24 May 2007, 377-377. https://doi.org/10.1109/ISI.2007.379513

[14] Aman, M.N., Javaid, U. and Sikdar, B. (2021) A Privacy-Preserving and Scalable Authentication Protocol for the Internet of Vehicles. *IEEE Internet of Things Journal*, **8**, 1123-1139. https://doi.org/10.1109/JIOT.2020.3010893

[15] Julien, F., Raya, M., Felegyhazi, M. and Papadimitratos, P. (2007) Mix-Zones for Location Privacy in Vehicular Networks. In Association for Computing Machinery (ACM) Workshop on Wireless Networking for Intelligent Transportation Systems

(WiN-ITS).
https://nss.proj.kth.se/publications/fulltext/location-privacy-mix-zones-vanet.pdf

[16] Huang, L., Matsuura, K., Yamane, H. and Sezaki, K. (2005) Enhancing Wireless Location Privacy Using Silent Period. In *IEEE Wireless Communications and Networking Conference*, New Orleans, 13-17 March 2005, Vol. 2, 1187-1192.
https://doi.org/10.1109/WCNC.2005.1424677

[17] Sheikh, M.S., Liang, J. and Wang, W. (2019) A Survey of Security Services, Attacks and Applications for Vehicular Ad Hoc Networks (VANETs). *Sensors*, **19**, 3589.
https://doi.org/10.3390/s19163589

[18] Lo, N.-W. and Tsai, H.-C. (2007) Illusion Attack on VANET Applications—A Message Plausibility Problem. In 2007 *IEEE Globecom Workshops*, Washington, 26-30 November 2007, 1-8. https://doi.org/10.1109/GLOCOMW.2007.4437823